

19 BUNDESREPUBLIK
DEUTSCHLAND



DEUTSCHES
PATENTAMT

12 Patentschrift
10 DE 195 16 992 C 1

21 Aktenzeichen: 195 16 992.1-51
22 Anmeldetag: 9. 5. 95
43 Offenlegungstag: —
45 Veröffentlichungstag
der Patenterteilung: 4. 4. 96

51 Int. Cl. 6:
B 60 R 25/00
B 60 R 25/04
E 05 B 49/00
E 05 B 65/12

DE 195 16 992 C 1

Innerhalb von 3 Monaten nach Veröffentlichung der Erteilung kann Einspruch erhoben werden

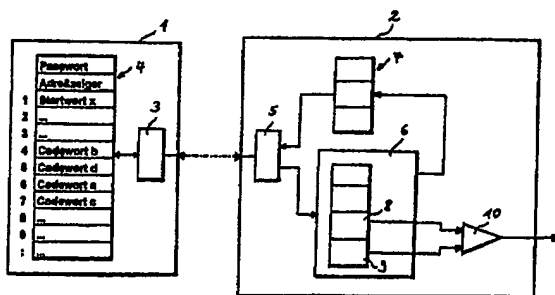
73 Patentinhaber:
Siemens AG, 80333 München, DE

72 Erfinder:
Pütz, Andreas, 51515 Kürten, DE

68 Für die Beurteilung der Patentfähigkeit
in Betracht gezogene Druckschriften:
DE 43 08 899 C1

64 Verfahren zum Betreiben einer Diebstahlschutzeinrichtung für ein Kraftfahrzeug und
Diebstahlschutzeinrichtung

57 Ein tragbarer Transponder (1) sendet zunächst ungültige
Daten zu einem Schloß (2), woraufhin ein Aufforderungssi-
gnal mit einer Speicheradresse zu dem Transponder (1)
zurückgesendet wird. Das im Transponder (1) unter der
Speicheradresse abgespeicherte Codewort wird ausgelesen
und zum Schloß (2) gesendet. Dort wird das Codewort mit
einem Sollcodewort verglichen. Bei Übereinstimmung wird
eine Wegfahrsperre freigegeben. Anschließend werden
Adresse und/oder Codewort im Schloß (2) neu berechnet
und im Transponder (1) für den nachfolgenden Freigabezy-
klus eingestellt. Somit entsteht ein Wechselcode.



DE 195 16 992 C 1

Die Erfindung betrifft ein Verfahren zum Betreiben einer Diebstahlschutteinrichtung für ein Kraftfahrzeug und eine Diebstahlschutteinrichtung, insbesondere eine Wegfahrsperrung.

Bei einer bekannten Diebstahlschutteinrichtung (DE 43 08 899 C1) findet zwischen einem Schlüssel und einem Schloß ein dreistufiger Dialog statt. Zunächst sendet der Schlüssel ein erstes Codesignal, das im Schloß mit Hilfe eines Rechners in ein zweites Codesignal moduliert wird. Das zweite Codesignal wird von dem Schlüssel empfangen, der seinerseits ein drittes Codesignal mit Hilfe einer Recheneinheit erzeugt, das zu dem Schloß zurückübertragen wird. Im Schloß wird das dritte Codesignal mit einem Sollcodesignal verglichen und bei Übereinstimmung wird eine Freigabesignal erzeugt.

Bei dieser Diebstahlschutteinrichtung ist im Schlüssel eine Recheneinheit notwendig. Nur so kann ein ständig wechselnder Code erzeugt werden.

Der Erfindung liegt das Problem zugrunde, ein Verfahren zum Betreiben einer Diebstahlschutteinrichtung für ein Kraftfahrzeug und eine Diebstahlschutteinrichtung zu schaffen, wobei in einem Schlüssel keine Recheneinheit vorhanden ist, und dennoch bei jeder Übertragung zwischen Schlüssel und Schloß bei jedem Freigabevorgang ein verändertes Codesignal übertragen wird.

Das Problem wird erfindungsgemäß durch ein Verfahren gemäß der Merkmale von Patentanspruch 1 und durch eine Diebstahlschutteinrichtung gemäß der Merkmale von Anspruch 5 gelöst.

Sobald ein Schlüssel ein Startsignal gesendet hat, wird im Schloß ein Aufforderungssignal erzeugt, wodurch der Schlüssel ein Codesignal seinem Speicher entnimmt, das zum Schloß gesendet wird. Im Schloß findet ein Vergleich mit einem Sollcodesignal statt. Bei Übereinstimmung wird ein Freigabesignal erzeugt. Im Schlüssel wird das Codesignal nicht errechnet, sondern durch das Schloß wird vorgegeben, unter welcher Adresse das Codesignal im Schlüsselspeicher zu finden ist. Nach jedem Freigabevorgang wird die Adresse und somit das Codesignal geändert.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen gekennzeichnet.

Ausführungsbeispiele der Erfindung werden anhand der schematischen Zeichnungen im folgenden näher erläutert. Es zeigen:

Fig. 1 ein Blockschaltbild der erfindungsgemäßen Diebstahlschutteinrichtung mit einem Schlüssel und einem Schloß,

Fig. 2a bis 2c ein Codesignalspeicher im Schlüssel bei einem ersten Ausführungsbeispiel und

Fig. 3a bis 3d ein Codesignalspeicher im Schlüssel bei einem weiteren Ausführungsbeispiel.

Eine erfindungsgemäße Diebstahlschutteinrichtung für ein Kraftfahrzeug weist einen tragbaren Schlüssel 1 auf (Fig. 1), der auf elektronischem Wege mit einem Schloß 2 im Kraftfahrzeug in Verbindung tritt. Im Schlüssel 1 ist eine Sende- und Empfangseinheit 3 angeordnet, über die Signale drahtlos übertragen und empfangen werden (in der Fig. 1 durch den gestrichelte Doppelpfeil dargestellt).

Über die Sende- und Empfangseinheit 3 gibt der Schlüssel 1 ein Signal ab, sobald er entweder ein Signal empfängt oder über die Sende- und Empfangseinheit 3 elektromagnetisch mit Energie versorgt wird. Der

Schlüssel 1 weist des weiteren einen Speicher 4 auf, in dem jeweils unter einer Adresse ein Codewort, z. B. Codewort a, Codewort b, usw., gespeichert ist. Ein Adreßzeiger zeigt jeweils auf die Adresse, unter der das jeweilige Codewort gespeichert ist, das anschließend gesendet wird. Überdies enthält der Speicher 4 einen Speicherbereich für ein fahrzeugspezifisches/benutzerspezifisches Paßwort.

Der Schlüssel 1 kann beispielsweise als Zündschlüssel oder Türschlüssel ausgebildet sein. Sobald der Zündschlüssel in das Zündschloß gesteckt wird, werden die Bauteile des Schlüssels 1 mit Energie versorgt. Daraufhin wird ein erstes Signal zu dem Schloß 2 übertragen.

Das Schloß 2 weist ebenfalls eine Sende- und Empfangseinheit 5 auf, die mit einer Recheneinheit 6 und einem Sendespeicher 7 verbunden ist. Die Recheneinheit 6 weist einen Empfangsspeicher 8, in den die empfangenen Signale eingeschrieben werden, sowie einen Sollwertspeicher 9 auf, in dem herstellerseitig oder benutzerseitig Sollwerte abgespeichert sind. Der Empfangsspeicher 8 und der Sollwertspeicher 9 sind mit einem Vergleich 10 verbunden, der bei Übereinstimmung der Inhalte der beiden Speicher 8 und 9 ein Freigabesignal an ein nicht dargestelltes Sicherheitsaggregat im Kraftfahrzeug sendet.

Ein solches Sicherheitsaggregat kann beispielsweise ein Steuergerät sein, das die Funktion einer Wegfahrsperrung erfüllt, wie beispielsweise ein Motorsteuergerät, ein Ventil zum Ab-/Zuschalten der Kraftstoffzufuhr oder ein Schalter zum Einschalten des Zündkreises. Durch eine Wegfahrsperrung ist nur bei Berechtigung ein Starten des Motors möglich. Als Sicherheitsaggregat können auch Türverriegelungen des Kraftfahrzeugs dienen.

Die Recheneinheit 6 ist mit dem Sendespeicher 7 verbunden in dem fahrzeugspezifische Paßworte, eine Speicheradresse sowie Codeworte gespeichert sind. Die Daten des Sendespeichers 7 werden über die Sende- und Empfangseinheit 5 zu dem Schlüssel 1 gesendet.

Ein erstes Ausführungsbeispiel des erfindungsgemäßen Verfahrens zum Betreiben einer Diebstahlschutteinrichtung wird anhand der Fig. 2a bis 2c näher erläutert.

In den folgenden Figuren ist jeweils der Speicher 4 dargestellt, der einen Paßwortspeicherbereich und Codewortspeicherbereiche aufweist. Ein Adreßzeiger zeigt gemäß einer Adresse, z. B. 1, 2, ... auf jeweils einen Speicherbereich, z. B. Startwort x, Codeworte b, ...

Zunächst zeigt der Adreßzeiger auf ein Startwort x (Fig. 2a). Auf dieses Startwort x zeigt der Adreßzeiger immer, wenn sich der Schlüssel 1 im Ruhezustand befindet.

Sobald der Schlüssel 1 von dem Schloß 2 aus induktiv mit Energie versorgt wird, wird ein Startsignal ausgesendet, das das Startwort x enthält. Mit dem Startsignal ist jedoch noch keine Freigabe des Sicherheitsaggregats möglich, da das Startsignal lediglich die Kommunikation zwischen Schlüssel 1 und Schloß 2 einleitet.

Das Startsignal wird von dem Schloß 2 empfangen, wodurch dort ein Aufforderungssignal erzeugt und ausgesendet wird. Das Aufforderungssignal kann einen fahrzeugspezifischen Paßwort, eine Speicheradresse und ein Codewort enthalten. Durch das von dem Schlüssel 1 empfangene Aufforderungssignal wird der Adreßzeiger auf die in dem Aufforderungssignal enthaltene Adresse gestellt, unter der das Codewort b (Fig. 2b) gespeichert ist. Nachfolgend wird dieses Codewort b in einem Codesignal zu dem Schloß 2 übertragen.

In dem Schloß 2 wird das empfangene Codewort b mit einem unter der gleichen Adresse in dem Sollwertspeicher 9 gespeicherten Sollcodewort verglichen. Bei Übereinstimmung der beiden Codeworte wird das Freigabesignal erzeugt und an ein Sicherheitsaggregat im Kraftfahrzeug gesendet. Bei Nichtübereinstimmung kann ein Alarm ausgelöst werden.

Danach wird nochmals ein Signal an den Schlüssel 1 gesendet, das das in dem Sendespeicher 7 gespeicherte Paßwort enthält. Wenn das gesendete Paßwort mit dem im Speicher 4 gespeicherten Paßwort übereinstimmt, kann der Adreßzeiger auf das Startwort x zurückgestellt werden. Ein Freigabezyklus ist somit beendet und der Schlüssel 1 befindet sich im Ruhezustand.

Wenn der Schlüssel 1 nun unberechtigterweise aktiviert werden sollte, so sendet er nur das Startwort x aus. Mit diesem Startwort x ist jedoch keine Freigabe der Wegfahrsperrung möglich. Dies kann nur durch ein gültiges Codewort, z. B. Codewort b, erfolgen.

Beim nächsten Freigabezyklus wird der Adreßzeiger abhängig von der empfangenen Adresse auf ein anderes Codewort, z. B. Codewort a oder c verstellt. Und zwar wird die neue Adresse im Schloß 2 durch einen Zufallsgenerator oder einen mathematischen Algorithmus erzeugt und zu dem Schlüssel 1 übertragen. Dementsprechend entsteht ein sogenannter Wechselcode, bei dem bei jedem Freigabezyklus ein vom vorhergehenden Codewort abweichendes Codewort übertragen wird. Erst nach einer bestimmten Anzahl von Freigabezyklen wiederholt sich das Codewort wieder. Wenn die Speicher 4, 7, 8 und eine sehr große Speicherkapazität haben, wird eine hohe Codevielfalt erzielt. Dann nutzt es einem Einbrecher auch nicht, wenn er das Codesignal abhört, denn beim nächsten Freigabezyklus führt ein anderes Codesignal zur Freigabe.

Ein weiteres Ausführungsbeispiel wird anhand der Fig. 3a bis 3d näher erläutert. Zunächst zeigt der Adreßzeiger auf die ungültigen Daten, d. h. auf das Startwort x, mit dem keine Freigabe des Sicherheitsaggregats möglich ist (Fig. 3a).

Sobald der Schlüssel 1 mit Energie versorgt wird, wird das Startwort gesendet. Daraufhin wird im Schloß 2 das Aufforderungssignal erzeugt, das ein Paßwort enthält. Wenn das Paßwort mit dem im Schlüssel 1 gespeicherten Paßwort übereinstimmt, wird der Adreßzeiger infolge des Aufforderungssignals auf das Codewort e versetzt (Fig. 3b). Durch einen vorangegangenen Freigabezyklus wurde dem Schlüssel 1 dieses Codewort e mitgeteilt.

Der Schlüssel 1 sendet daraufhin ein Codesignal, das dieses Codewort e enthält. Wenn dieses Codewort e mit einem unter der gleichen Adresse in dem Sollwertspeicher 9 gespeicherten Codewort übereinstimmt, wird das Freigabesignal erzeugt.

Anschließend wird mit Hilfe des Paßwortes ein neues Codewort in den Speicher 4 des Schlüssels 1 geschrieben. Hierzu wird in der Recheneinheit 6 ein neues, zufälliges Codewort zusammen mit einer Adresse erzeugt und in dem Sendespeicher 7 zwischengespeichert. Das Codewort und die Adresse werden zusammen mit dem Paßwort zu dem Schlüssel 1 übertragen. Nur wenn das gesendete Paßwort mit dem im Schlüssel 1 gespeicherten Paßwort übereinstimmt, wird der Adreßzeiger entsprechend der empfangenen Adresse verstellt und das neue Codewort (Codewort f wird mit dem Codewort k überschrieben) unter dieser Adresse gespeichert (Fig. 3c).

Somit wird dem Schlüssel 1 mitgeteilt, daß bei dem

nächsten Freigabezyklus dieses Codewort k ausgesendet werden muß. Somit weiß auch das Schloß 2, daß das beim nächstfolgenden Freigabezyklus unter dieser Adresse im Sollwertspeicher 9 abgespeicherte Sollcodewort mit dem empfangenen Codewort zu vergleichen ist.

Anschließend wird der Adreßzeiger wieder auf das Startwort x zurückgesetzt (Fig. 3d) und ein Freigabezyklus ist beendet. Sobald der Schlüssel 1 im Anschluß daran unberechtigterweise aktiviert wird, sendet er nur das ungültige Startwort x, mit dem keine Freigabe des Sicherheitsaggregats möglich ist. Ein Abhören des Startsignals durch Unberechtigte ist daher zwecklos.

Beim nächsten Freigabezyklus wird dann das unter der festgelegten Adresse abgespeicherte Codewort f gesendet. Das Codewort f wird vom Schloß 2 erwartet und dort mit demjenigen Codewort verglichen, das unter der gleichen Adresse im Sollwertspeicher 9 abgespeichert ist.

Anschließend wird das Codewort für den übernächsten Freigabezyklus festgelegt. Da die Adressen und Codeworte immer wieder neu mit Hilfe eines mathematischen Algorithmus oder durch einen Zufallsgenerator in der Recheneinheit 7 erzeugt werden, entsteht ein Wechselcode, bei dem sich bei jedem Freigabezyklus die Codeworte ändern. Je komplizierter der Algorithmus oder je aufwendiger der Zufallsgenerator aufgebaut ist, desto vielfältiger werden die Adressen/Codeworte und somit der Wechselcode.

Mit dieser erfindungsgemäßen Diebstahlschutzeinrichtung wird nur eine einzige Recheneinheit 6 im Schloß 2 benötigt, durch die der Wechselcode erzeugt wird. Als Recheneinheit 6 kann ein Mikroprozessor ein funktionsgleicher, kundenspezifischer integrierter Schaltkreis (ASIC) verwendet werden.

Im Schlüssel 1 genügt als Speicher 4 ein beschreibbarer oder programmierbarer Speicher, wie beispielsweise ein EPROM oder ein RAM. In dem Speicher 4 ist unter vorgegebenen Adressen jeweils ein Codewort abgespeichert, das dann abgerufen wird, wenn der Adreßzeiger gemäß der Adresse darauf zeigt. Ein bereits vorhandenes Codewort kann auch durch ein vom Schloß 2 übertragenes Codewort ersetzt, d. h. überschrieben, werden.

Die Signale werden zwischen dem Schlüssel 1 und dem Schloß 2 induktiv übertragen. Hierzu weisen die beiden Sende- und Empfangseinheiten Spulen auf, die dann transformatorisch, d. h. induktiv, zusammenwirken, wenn die beiden Spulen in unmittelbarer Nähe zueinander angeordnet sind.

Der "Schlüssel" weist die Sende- und Empfangseinheit sowie einen Speicher 4 auf. Der Schlüssel kann auch als Transponder bezeichnet werden. Der Schlüssel 1 kann von einem Benutzer getragen werden. Mit Hilfe des Schlüssels 1 findet eine elektronische Kommunikation mit dem Schloß 2 statt. Der Schlüssel 1 kann in Form eines mechanischen Schlüssels 1 oder als Chipkarte ausgebildet sein.

Das Schloß 2 weist die Sende- und Empfangseinheit, die Recheneinheit 6 und den Sendespeicher auf. Als Schloß 2 kann auch ein Steuergerät im Kraftfahrzeug verstanden werden, das die Signale von dem Schlüssel 1 empfängt, verarbeitet und das Freigabesignal erzeugt.

Unter dem Begriffen "Codewort" oder "Paßwort" werden codierte digitale Signale verstanden, die beispielsweise eine Länge von 16 Byte haben.

Durch den Adreßzeiger wird veranlaßt, daß ein durch die Adresse bestimmter Datenbereich des Speichers 4

ausgelesen und gesendet wird. Die Daten und zugehörigen Adressen sind sowohl im Speicher 4 des Schlüssels 1 als auch im Sollwertspeicher 9 identisch. Wenn im Schloß 2 zu Adressen gehörige Daten verändert werden, so werden sie auch durch Datentübertragung im Schlüssel 1 geändert.

Patentansprüche

1. Verfahren zum Betreiben einer Diebstahlschutzeinrichtung eines Kraftfahrzeugs, dadurch gekennzeichnet,

- daß ein Startsignal von einem Schlüssel (1) ausgesendet wird,
- daß das Startsignal von einem Schloß (2) empfangen wird, woraufhin ein codiertes Aufforderungssignal im Schloß erzeugt wird, das an den Schlüssel (1) zurücksendet wird,
- daß das Aufforderungssignal von dem Schlüssel (1) auf seine Berechtigung hin überprüft wird und bei Berechtigung abhängig vom Inhalt des Aufforderungssignals aus einem Speicher (4) ein Codesignal entnommen wird, das zu dem Schloß gesendet wird, und
- daß das Codesignal im Schloß (2) mit einem erwarteten Sollcodesignal verglichen wird und bei Übereinstimmung ein Sicherheitsaggregat freigegeben wird.

2. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß das Aufforderungssignal eine Adresse enthält, unter der in dem Speicher (4) des Schlüssels (1) jeweils ein Codesignal abgespeichert ist, wobei die Adresse bei jedem Aussenden des Aufforderungssignals gegenüber der vorher ausgesendeten Adresse verändert wird.

3. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß ein Adreßzeiger im Speicher (4) des Schlüssels (1) auf das Startsignal voreingestellt wird, durch das Aufforderungssignal auf die Adresse für das Codesignal verstellt wird und nach Aussenden des Codesignals wieder auf das Startsignal zurückgestellt wird.

4. Verfahren nach Anspruch 1, dadurch gekennzeichnet, daß mit dem Aufforderungssignal ein Paßwort und ein neues Codesignal an den Schlüssel (1) gesendet wird, wobei bei Übereinstimmung des Paßwortes mit einem Sollpaßwort das Codesignal unter einer Adresse in dem Speicher (4) des Schlüssels abgespeichert wird.

5. Diebstahlschutzeinrichtung zum Durchführen des Verfahrens nach Anspruch 1, gekennzeichnet durch

- einen Schlüssel (1), der einen Speicher (4) aufweist, in dem Codesignale unter Adressen abgespeichert sind und
- ein Schloß (2), das eine Recheneinheit (6), durch die nach Empfang eines Startsignals ein Aufforderungssignal erzeugt wird, und eine Vergleichseinheit (10) aufweist, die das empfangene Codesignal mit einem gespeicherten Sollcodesignal vergleicht und bei Übereinstimmung ein Freigabesignal an ein Sicherheitsaggregat sendet.

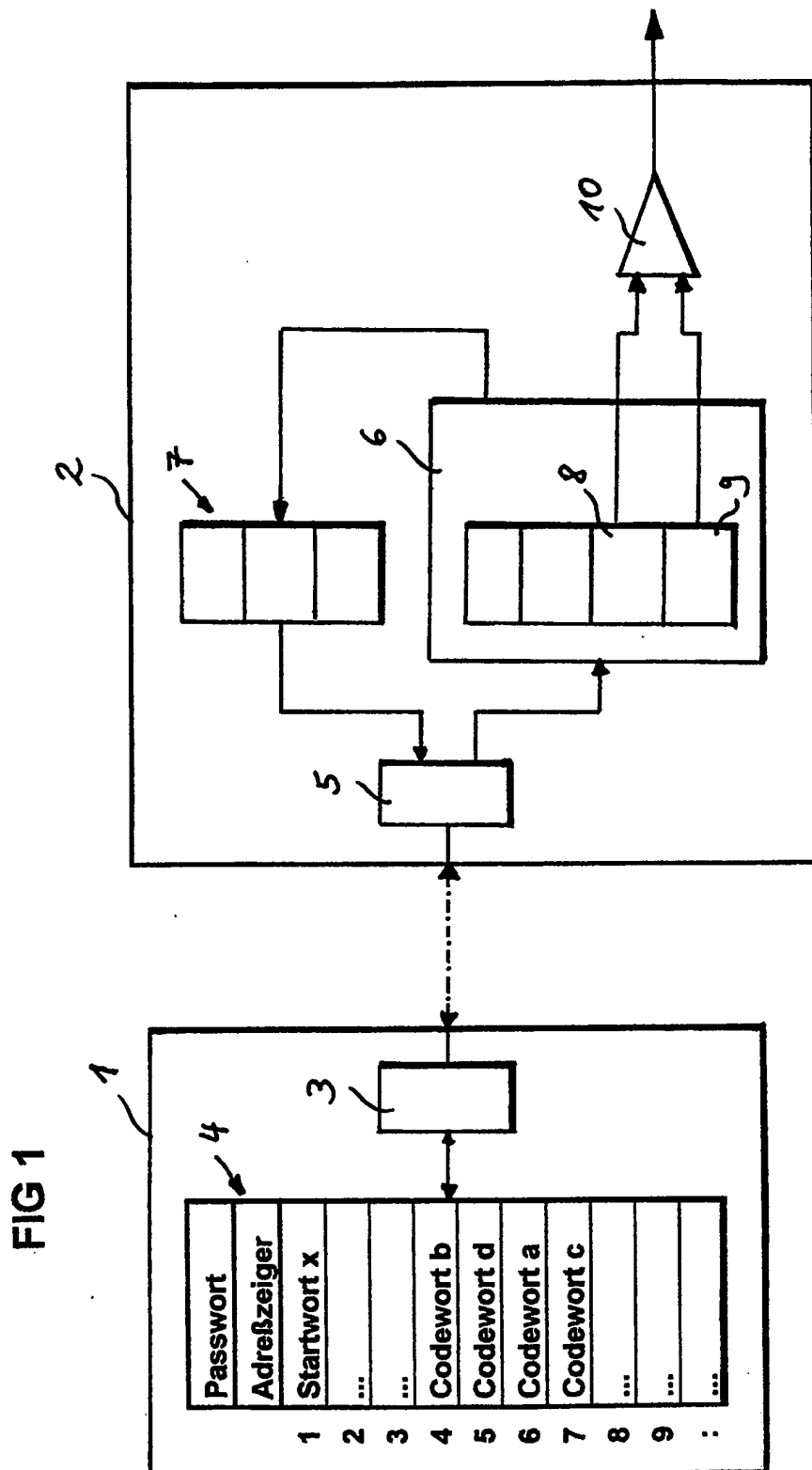
6. Diebstahlschutzeinrichtung nach Anspruch 5, dadurch gekennzeichnet, daß der Schlüssel (1) einen Transponder enthält.

7. Diebstahlschutzeinrichtung nach Anspruch 5, dadurch gekennzeichnet, daß das Sicherheitsaggregat

eine Wegfahrsperre oder eine Türverriegelung ist.
8. Diebstahlschutzeinrichtung nach Anspruch 5, dadurch gekennzeichnet, daß der Speicher (4) ein Schreib-/Lesespeicher ist.

9. Diebstahlschutzeinrichtung nach Anspruch 5, dadurch gekennzeichnet, daß Recheneinheit (6) ein Mikroprozessor ist.

Hierzu 3 Seite(n) Zeichnungen



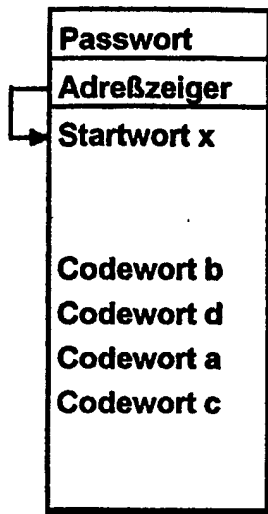


FIG 2a

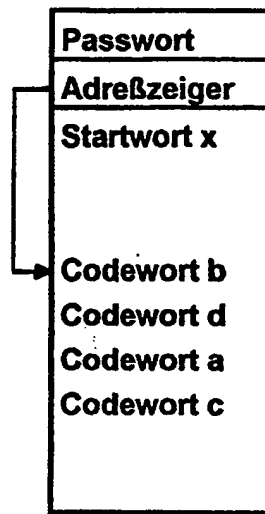


FIG 2b

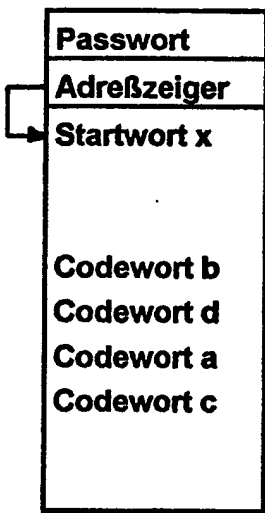


FIG 2c

